KRATOS®
SECUREINFO

FedRAMP: Six Major Challenges and Recommendations for Success

FedRAMP 3PAO Accredited SM

Kratos SecureInfo – Accredited FedRAMP℠ Third Party Assessor

Kratos SecureInfo Corporation is a market-proven provider of cybersecurity services and solutions with over 20 years of experience providing assessments and validations. Kratos SecureInfo is an accredited Third Party Assessment Organization (3PAO) under the Federal Risk and Authorization Management Program (FedRAMP) by the U.S. General Services Administration (GSA). The Kratos SecureInfo team is qualified to perform security assessments of Cloud Service Providers (CSP) to ensure they meet FedRAMP requirements.

INTRODUCTION

Since the introduction of the Federal Information Security Management Act (FISMA) a decade ago, system owners have invested millions of dollars developing millions of pages of documentation for certification and accreditation, and many millions more taking those systems through audits. For example, in 2009, John Streufert testified to Congress that "the Department [of State] spent $133M over the last six years amassing a total of 50 shelf feet, or 95,000 pages, of final Certification & Accreditation (C&A) documentation for about 150 major information systems."

With the growing importance of cloud-based solutions, the specter of imposing that regime on the providers brought about a re-think of the overall process: Federal Risk and Authorization Management Program (FedRAMP). Instead of every agency investing huge resources, the burden has been transferred to Cloud Service Providers (CSP) to invest in a single audited package to satisfy 110 major agencies, and reduce the enormous burden on organizations.

For several years, Kratos SecureInfo has worked with leading cloud providers to advise and guide them through the preparation, testing, and demonstrated compliance necessary to do business with the federal government. Whether for infrastructure, platform, or software as a service, the challenges of compliance loom large. The key to success is a knowledgeable partner with battle-hardened experience.

Kratos SecureInfo has identified six lessons learned. These lessons can reduce scheduling delays, and increase opportunities for efficiencies for providers and agencies. This paper presents a sampling of six audit best practices that promote a more cost-effective and sustainable Authorization to Operate (ATO) lifecycle for CSPs.

SIX MAJOR FEDRAMP CRITICAL SUCCESS FACTORS

The issues that plague a cost effective acquisition of the FedRAMP ATO won't be a surprise to most Program Managers. What may surprise them are the nuances of how and why these issues significantly impact bringing cloud services to market, the symptoms of each issue, and how to resolve them.

Assessing a cloud implementation for the symptoms of these issues should occur continuously throughout the ATO acquisition and renewal process. Ignoring the symptoms of these issues increases ATO life cycle costs and threatens the existence and any associated sunk costs in the CSP offering. The six critical success factors and the methodologies for achieving them include:

- Accurate system boundary definitions

KRATOS SECUREINFO

- Correct and complete system inventory
- Appropriate sampling methodologies
- Effective vulnerability testing
- Identification of time-critical key control vulnerabilities
- Identifiers, authentication and multifactor authentication

Accurate System Boundary Definitions

Problem Definition

The complexity of a cloud environment makes the boundary definition process more challenging and it is not resolvable with just a list of physical assets. The difficulty in creating an accurate system boundary has both business as well as technical impacts. The business impact of not initially identifying an accurate system boundary causes ATO delays that translate into lost opportunity costs and higher life cycle costs. Some of the technical impacts of not identifying an accurate system boundary include:

- Inaccurate/ambiguous reporting of the asset inventory and any associated controls of those assets,
- Incomplete vulnerability testing and Plan of Action and Milestone (POA&M) creation – significantly impacting service life cycle costs,
- Incomplete or inaccurate assessment of data and associated sensitivity requirements (Inaccurate high sensitivity requirements artificially increase service life cycle costs,
- Incomplete or incorrect control-owner identification and
- Potential for incomplete or inaccurate external interface information.

Defining a boundary has several variables that increase the complexity:

- Dynamically adjusting resources in single or multi-tenant environments,
- Conflation of logical versus physical assets in a dynamic environment of virtual machines,
- Dynamic adjustments for computational allocations and storage and
- Replication of information assets across system boundaries due to data redundancy algorithms.

The acquisition of either the initial ATO or subsequent re-certifications is made more difficult when there is an unexplained discrepancy between artifacts such as the system boundary definition and system inventory. This means that any perception of a discrepancy between the artifacts discovered during the third party audit as well as in the ATO review process must be clarified preemptively, before schedule or technical impacts occur. For example, if a significant discrepancy

between the boundary definition and inventory exists in the ATO authorization package, additional vulnerability scanning may be mandated and result in a re-submittal of the ATO authorization package. This delay and increased level-of-effort has a price tag attached to it, impacting the service life cycle costs and profit margin, and it may impact public relations efforts or the corporate image.

Potential Resolution

Kratos SecureInfo's approach to accurately developing a system boundary definition is to triangulate the boundary from several data sources through the use of best-practice exercises.

- Map out data flows across physical, network, system, and application layers including all inputs, outputs, and data transformations.
- Identify all upstream and downstream data consumers.
- Illustrate logical boundary diagrams across multiple views (i.e., data flow view, data access view, system interconnections view, physical cross connections view).
- Map out logical components within the physical components.
- Document all boundary exclusions along with associated justifications and evidence.
- Obtain consensus among system owner(s), ISSO(s), and assessors.

Accurate and Complete System Inventory

Problem Definition

System inventories in larger cloud providers can change by the minute. The discovery of additional components during testing can cause delays in testing activities to rationalize and account for the asset discrepancies. Delays in testing can disrupt the schedule and increase the assessment level-of-effort for all parties involved. Both schedule interruptions and increasing the assessment level-of-effort leads to unnecessary increases in the ATO assessment lifecycle costs. Consequently, it is critical to capture an accurate system inventory that is as current as possible prior to the actual testing window.

Potential Resolution

There is a two-step methodology in reporting an accurate and complete system inventory. First, procedures must be developed to ensure that inventory reports used for ATO are taken as a point-in-time snapshot that is combined with electronic discovery scans to converge on the most accurate inventory information available. Ideally, the inventory should be sources from an automated asset management system.

Secondly, a strategy that works especially well for larger providers is to take an iterative approach to system inventory. Early inventory

KRATOS SECUREINFO

data-calls help assessors become oriented to systems and technologies in use by location, logical zone, and role. The repetitive nature of the inventory data-call process familiarizes the CSP staff with the use of the internal processes required to accurately and consistently pull inventories for ongoing continuous monitoring and reporting needs. The end product is a staff trained in an evolved system inventory procedure, resulting in a greater point-in-time reporting accuracy.

Appropriate Sampling Methodologies

Problem Definition

Attempting to assess every device and virtual machine within the system boundary—especially for large CSPs—is impractical. It is safe to say that the general goal of CSPs is to provide accurate and cost-effective methods of sampling devices and virtual machines within a cloud system boundary during the third-party audit process. A sampling methodology needs to be devised that takes into account devices, hypervisor instances and virtual machines based on system role, configuration management standards, data sensitivities, and levels of access. Based on data center design (i.e., modular container designs), it may even make sense to sample facilities.

Potential Resolution

As a Third Party Assessment Organization (3PAO), one of Kratos SecureInfo's goals is to decrease potential impacts on the assessment schedule by submitting the sampling methodology to the Joint Authorization Board (JAB) as early as possible. In addition, the following evolved sampling methodology provides a cost-effective and accurate assessment:

- Obtain and review a current asset inventory list that contains descriptive details on asset role, location, version, configuration, technology, access, sensitivity, and owner,
- Gain an inventory of virtual machine images, versions, and configurations,
- Access hypervisor configuration(s) including resource controllers, and load/storage algorithms,
- Review the configuration management plan and practices to identify commonly used device, virtual machine, and hypervisor profiles,
- Identify integrity mechanisms to validate configuration management practices,
- Document a sampling methodology that may range between 5-10% of system type based on role plus virtual machine images,
- Execute sample testing,
- Map the sample testing against the inventory and the security controls and configurations specified in the System Security Plan (SSP). Check for discrepancies between these sources to verify accuracy and the efficacy of the methodology and
- Submit the Sampling Methodology to JAB.

KRATOS SECUREINFO

Effective Vulnerability Testing

Problem Definition

It is critical to design a testing approach that can provide an accurate picture on the system's security posture and also not generate a high number of false positives. Unfortunately, accuracy is not a forgone conclusion. Popular vulnerability scanners such as Nessus®, Retina® or Foundstone Scanner® do not produce scanning plug-ins for proprietary operating systems as well as the custom hypervisors that reside on top of the OS kernel. Additionally, database scanners such as AppDetective® can incorrectly characterize a cloud service database instance and never complete the scanning process or the effort may yield numerous false positives.

Using traditional electronic testing approaches often results in a series of well-known discovered service ports that do not correlate with actual production systems and virtual machines. These inaccurate test results can create unnecessary confusion when comparing scanning data to system inventory data, the System Security Plan (SSP) or even the list of known POA&MS. This confusion can lead to an increased level-of-effort in the third-party assessment process as well as in the review and granting of the ATO. The increased level-of-effort usually results in higher costs.

Potential Resolution

Developing accurate vulnerability scans and penetration tests often involves intensive technical collaboration between the CSP and the assessors. To promote accuracy as well as efficiency, the third-party assessor and the operational staff of the CSP need to coordinate in the following ways:

- Conduct technical workshop(s) with the CSP's security operations staff to understand current vulnerability management practices,
- Review historical penetration testing and vulnerability scanning reports,
- Determine appropriate locations of network access that may yield the most thorough and accurate results.
- Identify who will be responsible for running vulnerability scans and what their turn-around will be,
- If necessary, design custom test harnesses to tunnel/route/throttle vulnerability test traffic to the correct source and destination, correct source and destination,
- Identify windows of testing time where environment changes occur at the lowest rate,
- For systems that cannot be checked electronically, conduct system configuration inspections using Center for Internet Security (CIS) and/or National Security Agency (NSA)

KRATOS SECUREINFO

benchmarks for technology guidelines that most closely resemble the cloud environment,
- As needed, develop custom scripts to pull system configurations that can only be run as read-only,
- Conduct manual tests for susceptibility to cross-site scripting, cookie and DNS poisoning, and SQL injection, etc. to determine exposure to attacks at the application and database layers,
- Develop Standard Operating Procedures(SOP) and scripts for all test staff on the methods for receiving, processing and reporting of scanned data into the FedRAMP Security Assessment Report (SAR) tables,
- Review electronic test results with the CSP to flesh out false positives and remediation items and
- Map test results to appropriate point-in-time snapshots of the system inventory.

Identification of Key Control Vulnerabilities Requiring a Long-Term Remediation Process

Problem Definition

Key controls that require remediation can impact the entire process and schedule. Often those remediation activities that require engineering (i.e., multi-factor authentication, robust auditing, and FIPS 140-2 crypto) are critical dependencies in completing successful assessment projects. These critical dependencies occur because CSPs need to identify remediation activities as new features or enhancements. New features or enhancements need configuration management control and usually require one or more iterations of a systems development lifecycle to complete. While rapid development methodologies can shorten the remediation timeline, there is a secondary impact as to whether a version change is considered significant enough to restart the security authorization cycle.

Operational delays in providing services and tracking/monitoring remediation activities will impact security assessment life cycle costs. Kratos SecureInfo has evolved a triage approach for minimizing the impact on the assessment schedule of key control remediation requirements.

Potential Resolution

Kratos SecureInfo recommends that the following approach be used to minimize the impact of critical dependencies and escalated costs in completing successful assessment projects:

- Assessments should commence with an identification process of partially or non-implemented controls that may have an engineering impact,
- Prioritize the assessment activities for the list of partially or non-implemented controls to segregate operational impact control failures first and document control failures last and

- Engage development lifecycle resources to obtain accurate estimates for completion so that timelines can be synchronized and duplicate effort eliminated.

This approach can augment the traditional risk based method to provide CSPs and the JAB with two different dimensions of POA&M: estimates-to-completion and POA&M impact level.

Identifiers, Authentication and Multifactor Authentication

Problem Definition

By definition, all CSPs are multi-tenant organizations, and this means that identification, authentication, and authorization are critical lynchpins to the security of their systems. FedRAMP requires comprehensive and well-implemented multifactor authentication (MFA). For FedRAMP, MFA must be implemented for not only remote access methods, but also local network access, and even physical access wherever possible.

FedRAMP compliant MFA becomes a challenge for those CSPs that have grown organically and either intermingle their administrative users in the same infrastructure with their customers, or place their administrative users into an enterprise-wide solution like Active Directory. Unfortunately, each approach brings with it certain vulnerabilities.

For those CSPs that have adopted an architecture with comingled users, becoming FedRAMP compliant requires extra precautions to ensure that the two user bases—with vastly different access levels—are kept fully isolated. For those CSPs that have adopted an enterprise approach, storing users can bring with it even more challenges. First, the enterprise approach is often used for a large number of systems with very different security postures. These different security postures can introduce vulnerabilities to the resources of the service as well as to the client population. Second, including the enterprise system in the assessment can both increase scope, risk and therefore ATO life cycle costs, as well as potentially increase internal process hurdles. Finally, due to other system requirements, an enterprise system simply may not be able to meet the strict requirements of the FedRAMP process.

Potential Resolution

Based on extensive cloud experience, Kratos SecureInfo believes that the most cost-effective and long-term maintainable solution has a minimal number of entry points through the system boundary, where each entry point is protected by MFA. By reducing the number of entry points, this makes the evaluation easier, and more importantly the security simpler to implement. Examples of entry points include bastion hosts, sometimes called jump boxes, and perimeter VPN solutions.

Also, MFA needs to be implemented with as clear a boundary as possible on every administrative interface, ensuring there is a simple story to explain its implementation and use. Lastly, MFA must be available to all customers for use in managing their cloud environment. In Kratos SecureInfo's experience, a self-contained implementation, separate from the administrative deployment mentioned previously, is preferable.

Once the solution is in place, other options, such as directory federation, can be examined. Federation allows a customer to assume the responsibility for management of accounts and MFA. This allows government customers to implement solutions that are both familiar and trusted.

CONCLUSION – A CALL TO ACTION

FedRAMP represents a brave new world for CSPs and the Federal government, one that brings potential rewards for everyone involved. In order to maximize the benefits for CSPs and government customers, experience is required to navigate the new challenges; experience that Kratos SecureInfo has developed. To find out more about how your organization can reduce lifecycle costs and streamline the FedRAMP process, contact us at at 1-888-677-9351, email Support@SecureInfo.com or visit www.secureinfo.com.

About Kratos SecureInfo

Kratos SecureInfo is Kratos' dedicated business group of cybersecurity professionals providing comprehensive cybersecurity solutions to a range of industries, with particular specialties in government, healthcare, energy and other critical infrastructure markets. Kratos SecureInfo addresses all aspects of the information security spectrum - from cloud security and continuous monitoring to risk management and compliance. Kratos SecureInfo is an accredited FedRAMP Third Party Assessment Organization (3PAO), an independent Agent of the Certifying Authority (ACA) for the United States Air Force and a corporate member of the Healthcare Compliance Association.

KRATOS SECUREINFO